SIKKIM

GOVERNMENT GAZETTE

EXTRAORDINARY
PUBLISHED BY AUTHORITY

Gangtok **Wednesday 21st June, 2023** **No. 230**

DIRECTORATE OF SIKKIM STATE LOTTERIES
FINANCE DEPARTMENT
GOVERNMENT OF SIKKIM
GANGTOK.

No. FIN/DSSL/III/960/2023-24/199 **Dated: 21/06/2023**

NOTIFICATION

In pursuance of sub-rule 13 of Rule 28 of the Sikkim Casino Games (Regulation) Rules, 2007, bearing Notification No: 02/TD dated 20/04/2007 published in Official Gazette bearing No: 154 dated the 21st of April, 2007, read with sub-rule (*7*) of rule 9 of the Prevention of Money – Laundering (Maintenance of Records) Rules, 2005, the State Government hereby makes the following guidelines, namely:—

1. ***Short title and commencement.***—

(*1*) These guidelines may be called the Sikkim Anti Money Laundering and Combating of Financial Terrorism Guidelines, 2023.

(*2*) They shall come into force at once.

2. ***Definitions.***— (*1*) In these guidelines, unless the context otherwise requires,—

(*a*) "Act" means the Prevention of Money- Laundering Act, 2002 (Central Act 15 of 2003);

(*b*) "beneficial owner" means natural person who ultimately owns or controls a client and/or the person on

whose behalf a transaction is being conducted;

(*c*) "Government" means the Government of Sikkim;

(*d*) "rules" means the Prevention of Money – Laundering (Maintenance of Records) Rules, 2005.

(*2*) Words and expressions used in these Guidelines and not defined, but defined in the Act and/or Rules, shall have the meaning respectively assigned to them in the Act and/or rules, as the case may be.

3. ***Objectives.***—

(*1*) The objective of these Guidelines is to prevent casinos from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. Know Your Customer (KYC) procedures also enable casinos to understand their customers and their financial dealings better which in turn help them manage their risks prudently.

(*2*) The objective of these Guidelines is to explain and expand the obligations of casino and its employees in discharging their responsibilities under the Act.

4. ***Money laundering and financing of terrorism.***—

(*1*) Money laundering involves disguising financial assets so that they can be used without detection of the illegal activity that produced them. Through money laundering, the monetary proceeds derived from criminal activity are transformed into funds with an apparently legal source.

(*2*) There is no one single method of laundering money. Despite the variety of methods employed, the laundering process is generally accomplished in three stages, which are as follows:—

(*a*) ***Placement*** – the physical disposal of cash proceeds derived from illegal activity;

(*b*) ***Layering*** – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity; and,

(*c*) ***Integration*** – the attempt to legitimize wealth derived from criminal activity. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as legitimate funds.

5. ***Money-Laundering through Casinos.***—

Terrorists and terrorist organizations require funds to carry out their activities. While they may not be keen to disguise the origin of their money, they are interested in concealing the destination and the purpose for which the money was collected. Terrorists and terrorist organizations, therefore, employ techniques similar to money launderers to hide and disguise the money. Examples of money laundering methods and techniques involving casinos are as under:—

(*a*) ***Use of illicit funds to gamble***:

This is the simplest method of gambling illicit funds in the hope of generating certifiable winnings. The money launderer will then receive a casino cheque for the total amount of credits remaining on the machine plus the jackpot.

(*b*) ***Buying winnings from legitimate customers***:

Money launderers approach customers who have won gaming machine jackpots, or accumulated a large amount in casino chips from winnings on table games and offer them cash at a premium above their winnings.

(*c*) ***Parallel Even money betting:***

In cases where gambling is undertaken to launder funds, it is usually on low odds, low risk games, such as, the even money options on roulette. This would involve two or more

persons placing opposite equivalent bets on even money wagers in the same game. The bet is 'double or nothing'. In this case the winning party could be paid out with a winnings cheque.

(*d*) ***Betting against associates /intentional losses***:

A number of casino games provide money launderers the option to bet against an associate so that in most cases one party will win. As a result of the money launderer's intentional losses, the associate is able to receive a casino issued cheque of 'legitimate' winnings.

(*e*) ***Use of Casino Value Instruments***:

Casinos utilize various value instruments to facilitate gambling by their customers. Casino chips are issued by casinos and used in lieu of cash in gaming transactions between the house and players. Chips are marked with the denomination and are negotiable within the casino. The illegal proceeds can also be used to purchase other casino value instruments like 'casino gift certificates' or 'casino reward cards'.

(*f*) ***Structuring***:

Structuring or smurfing involves the distribution of a large amount of cash into a number of smaller transactions in order to minimize suspicion and evade Know Your Customer (KYC) and threshold reporting requirements.

(*g*) ***Refining***:

Launderers pay low denomination cash into their casino accounts and withdraw funds with cash of higher denominations. This facility can be used to exchange notes linked to crime with clean notes.

(*h*) ***Use of Casino Accounts facilities***:

Many casinos offer deposit accounts and lines of credit with less scrutiny and Customer Due Diligence (CDD) requirements than financial institutions. The frequent movement of funds between financial institutions and casinos, or between casino accounts held in different casinos may be vulnerable for money laundering.

(*i*) ***Conversion of large sums of foreign currency***:

If casinos offer currency exchange services, launderers may use large, one-off, or frequent foreign currency exchanges or deposits of a foreign currency.

(*j*) ***Use of Credit/Debit cards***: Many casinos allow customers to purchase casino chips using credit cards. The outstanding credit card balances are paid by the card holder at the bank using the illicit funds. However, criminal's use of credit cards provides an opportunity for authorities to follow the money trail more readily.

6. As per the provisions of section 12 of the Act, every banking company, financial institution and intermediary has an obligation to verify the identity of its clients, maintain certain records and furnish certain information to the Director, Financial Intelligence Unit-India (FIU-IND). The rules prescribe the manner in which identity of clients is to be verified, nature of information record which has to be maintained and furnished to Director, Financial Intelligence Unit, India (FIU-IND) and manner in which records have to be maintained. Casinos are covered under the category of financial institutions and are liable for all these obligations which are explained briefly in the following clauses.

7. ***Obligations of Casinos***:-

(*a*) Every casino shall prepare its Know Your Customer/Anti Money Laundering/Combating Financing of Terrorism Policy and procedures aimed at preventing and detecting money laundering and terrorist financing.

(b) The rules require appointment of a person as Principal Officer by each casino and hence casinos shall appoint a senior management officer as Principal Officer and inform his particulars to Financial Intelligence Unit, India. The Principal Officer shall act as a central reference point of the casino for the purpose of interaction with Financial Intelligence Unit, India and shall ensure that the obligations under the Act and Rules are fulfilled.

(*c*) Casinos shall ensure that the Principal Officer is able to act independently and report directly to the senior management or to the Board of Directors. The Principal Officer shall be located at the head/corporate office of the casino and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law.

(*d*) The role and responsibilities of the Principal Officer shall include overseeing and ensuring overall compliance with regulatory guidelines on Know Your Customer/Anti Money Laundering/Combating Financing of Terrorism issued from time to time and obligations under the Act, Rules and Regulations made thereunder, as amended from time to time. The Principal Officer shall also be responsible for timely submission of prescribed reports to Financial Intelligence Unit, India.

(*e*) With a view to discharge his responsibilities effectively, the Principal Officer and other appropriate staff shall have timely access to customer identification data and other Customer Due Diligence information, transaction records and other relevant information.

(f) ***Verification of Identity of Customer.***—

(i) Casinos shall verify the identity of its customers who engage in financial transactions equal to or exceeding the prescribed threshold, whether conducted as a single transaction or several transactions that appear to be connected. Financial transactions in casinos include the purchase or cashing in of casinos chips or tokens, the opening of accounts, wire transfers and currency exchanges. Financial transactions do not refer to gambling transactions that involve only casino chips or tokens.

(ii) If a casino has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the prescribed threshold, the casino shall verify and identity the address of the customer and also consider filing a Suspicious Transaction Report (STR) to the Financial Intelligence Unit, India.

(*iii*) If the casino has an account-based relationship, the casino shall identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship at the commencement of relationship.

(*iv*) Casinos shall determine whether a client is acting on behalf of a beneficial owner, identify the beneficial owner and take all reasonable steps to verify his identity.

(v) The identity of a client shall be verified by the casinos from an "officially valid document". Officially valid document as defined in rule 2(*1*)(*d*) of the Rules which includes passport, driving license, Permanent Account Number (PAN) Card, Voter's Identity Card issued by Election Commission of India, job card issued by National Rural Employment Guarantee Act (NREGA) duly signed by an officer of the

Government, letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number, etc.

(*vi*) Casinos shall develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the aspects of customer relationship in the casino.

(*vii*) Casinos shall not allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified

(*viii*) Conducting customer identification at the entry to a casino is not sufficient. Casinos shall ensure that they are able to link customer due diligence information for a particular customer to the transactions that the customer conducts in the casino.

(*ix*) When there is suspicion of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained identification data in respect of regular customers, casinos shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship.

(*x*) The Board of Directors of the casino shall ensure that an effective Know Your Customer programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility shall be explicitly allocated within the casino for ensuring that the casino's policies and procedures are implemented effectively.

8. ***Identification and assessment of risk.***—

(*a*) Based on its own criteria, a casino shall seek to determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. Categories of Customers whose activities may indicate a higher risk include:—

(*i*) ***Politically exposed persons***: Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior Government/judicial/military officers, senior executives of state owned corporations, important political party officials, etc. Casinos shall gather sufficient information on any customer of this category intending to establish a relationship and check all the information available of the customer in the public domain. Casinos shall verify the identity of the customer and seek information about the sources of funds before accepting the Politically Exposed Person (PEP) as a customer.

(*ii*) ***High spenders***: Given the variations among casinos, the level of spending considered to be relatively high for an individual customer will vary among operators, and even among casinos owned and managed by the same operator. Customers may become high spenders because of their cumulative spending over a period of time (e.g. customers with relatively high level of spending with casino account holder relationship). Similarly, casual customers who gamble a relatively large amount of money on a limited number of occasions, perhaps even during a single visit, could equally be considered as high spenders.

(*iii*) ***Disproportionate spenders***: Casinos shall devise policies relative to obtaining information about customers' financial resources, when feasible and available, to determine if customers fall into this category. Regular customers may pose a risk, particularly if their spending pattern changes, e.g. it dramatically increases or their rated play does not fit their playing profile e.g. minimal play.

(*iv*) ***Improper use of third parties***: Terrorists and terrorist organizations may use third parties, or anonymous or identified agents to avoid Customer Due Diligence undertaken at a threshold. They may also be used to gamble, e.g. to break up large amount of cash. Third parties may be used to buy chips, or to gamble on behalf of others with minimal play (which may include early or high cash outs), or cash out/ redeem chips for larger denomination currency, casino checks, etc.

(*v*) ***Junkets***: Junket operators that provide premium players are known to exert pressures on casinos for reducing scrutiny of individual spending patterns, or may try to unduly influence or exercise control over licensed casino operations. Further, junket organisers may engage in lending or the facilitation of lending to players outside casinos' knowledge. In addition, junket organisers may allow to 'pool' and therefore obscure the spending of individual customers, thus preventing casinos from making any assessment of customers' spending patterns. The junket operators may supply players of unlicensed sub-junket operators who can act as unlicensed collectors of credit and may have ties to organized crime networks. Consequently, casinos would need to devise measures to identify and prevent junket organisers from engaging in informal arrangements that are inconsistent with risk-based Anti Money Laundering/Combating Financing of Terrorism policies, procedures and internal controls.

(*vi*) ***Customers with multiple casino player rating accounts***: Some players may open up multiple player rating accounts with different names at the same casino and may provide different rating account numbers to casino at different times to hinder a casino's ability to track their gambling activities under the same customer name. Casinos need to identify such accounts with similar players' names and the same physical descriptions (e.g. age, male or female, eye colour, hair colour, height, weight) to be able to monitor customers' aggregate gambling across their casino business. Casinos shall implement policies, procedures, and systems to assist in the identification of customers opening multiple-player rating accounts for dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid reporting thresholds.

(*vii*) ***Unknown Customers***: Unknown customers that purchase large amounts of chips with Currency at table games, engage in minimal or no play, and then redeem the chips for large denomination bills, casino cheques or money/wire transfers are also high risk.

(*b*) Casinos shall not accept a customer where the casino is unable to apply appropriate customer due diligence measures i.e. casino is unable to verify the identity and/or obtain documents required as per the risk categorisation due to non co-operation of the customer or non-reliability of the data/information furnished to the casino. It is, however, necessary to have suitable built in safeguards to avoid harassment of the customers.

(*c*) Casinos shall consider operational aspects (i.e. products, services, games, and accounts/ account activities) that can be used to facilitate money laundering and terrorist financing activities. Casinos have the following potential transaction risks:

(*i*) ***Proceeds of crime***: Customers may use casinos for transferring money gained from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer. Paying greater attention to high spenders/rollers will be helpful in mitigating this risk.

(*ii*) ***Cash***: Customers may use casino to exchange large amounts of illicit proceeds denominated in small bills for larger ones that are easier to hide or transport.

(*iii*) ***Transfers between customers***: If casinos wish to allow inter-account transfers between their customers they shall devise careful policies and procedures which monitor the amount of the transfer(s).

(*iv*) ***Borrowing***: Casinos may also be aware of customers borrowing money from non-conventional sources, including other customers. Informal money lending can be illegal, and it can also offer terrorists an opportunity to introduce proceeds of crime, usually cash, into the legitimate financial system through the casino.

(*v*) ***Loan Sharking***: Casinos may also be aware of loan sharking which involves lending money to individuals at an interest rate that is above a maximum legal rate, sometimes collected under threat of violence.

(*d*) Casinos shall also take into account risks arising from high risk jurisdictions or countries. The indicative list of high/medium risk jurisdictions is as under:

(*i*) Countries subject to sanctions, embargos or similar measures in the United Nations Security Council Resolutions ("UNSCR").

(*ii*) Jurisdictions identified in Financial Action Task Force public statement as having substantial money laundering and terrorist financing (ML/FT) risks (www.fatf-gafi.org).

(*iii*) Jurisdictions identified in Financial Action Task Force public statement with strategic Anti Money Laundering/Combating Financing of Terrorism deficiencies (www.fatf-gafi.org).

(*iv*) Countries identified by the casino as high-risk because of its prior experiences, transaction history, or other factors (e.g. legal considerations, or allegations of official corruption).

9. ***Internal controls and monitoring obligations.***—

(*a*) Casinos shall implement appropriate measures and controls to mitigate the potential money laundering risk.

(*b*) Casinos shall develop and implement a framework of internal controls (e.g. policies, procedures and processes) for all operating divisions and departments reasonably designed to safeguard operations against money laundering and terrorist financing. Anti Money Laundering/Combating Financing of Terrorism internal controls shall cover all related activities and programs such as suspicious activity reporting, cash transaction reporting, customer identification, casino recordkeeping, records retention, and compliance. Internal controls shall also include documentation procedures and management information/monitoring systems adequate to detect and report suspicious activity in a timely manner to authorities. In addition, internal controls shall mitigate the inherent risk of any high-risk customer, product, or service as well as transactions to or from a high-risk country that could be misused for money laundering or terrorist financing.

(*c*) Senior management shall ensure that their ownership of the Anti Money Laundering/ Combating Financing of Terrorism issue is visible at the Board or equivalent level and to

all staff and business partners, including acknowledging their personal responsibility to ensure that there are adequate systems and controls in place. The management shall encourage a culture of compliance.

(*d*) The internal controls implemented by casino shall be commensurate with:—

(*a*) complexity, organisation, and relative size of the business;

(*b*) risks posed by the types of gambling and financial services offered as well as the volume of business; and

(*c*) risks posed by the types of customers and geographical location.

(d) Casinos shall enhance due diligence requirements for high risk customers which may require information about the source of funds and taking management's approval before doing business.

(*e*) Monitoring methodologies and processes need to take into account the resources of the casino. Casinos that have surveillance departments use video recording media and maintain records that identify customer activity and shall also include monitoring potential suspicious transaction reporting. Casino may use its surveillance system to assist it in monitoring customers who are conducting financial transactions which are unusual, suspicious, or potentially criminal in nature.

(*f*) Casinos may also consider barring customers because of false identification, inadequate identification; or suspicious transactions.

(*g*) Casinos shall exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds.

(*h*) Casinos shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Casinos may prescribe threshold limits and pay particular attention to the transactions which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer shall particularly attract the attention of the casino.

(*i*) Casinos shall pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

(*j*) Casinos shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in Financial Action Task Force Statements and countries that do not or insufficiently apply the Financial Action Task Force Recommendations. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions shall, as far as possible be examined, and written findings together with all documents shall be retained and made available to relevant authorities, on request.

(k) Casinos shall have policies, procedures, and internal controls to identify large redemptions to such a customer that were paid with currency (including any large cash outs without gambling for large denomination bills), or through issuance of a cheque.

(*l*) Casinos shall implement procedures and systems to assist in the identification of unknown customers redeeming large amounts of chips for dishonest or inappropriate

reasons, including attempting to obscure their spending levels, or to avoid checks undertaken at a threshold level. This could extend to measures such as not cashing out such customers or cashing out by paying in small denomination bills, which are harder to hide or transport, as well as maintaining surveillance photographs and filing suspicious activity reports with physical descriptions.

(m) As part of a casino's risk-based prevention program, when a customer presents at a cage a large chip or token redemption, a cashier shall confirm it typically by a telephone call to a pit boss, floor person, card room supervisor, or other casino employee to determine if the chips were put at risk, or won at a table game as "verified winnings" or purchased at a table (e.g. when a customer is "walking with" chips at the end of table game play) to identify:

(*i*) potential counterfeit chips or tokens,

(*ii*) stolen chips or tokens, or

(*iii*) any temporary advance of chips to a customer. Also, a cage cashier shall query a casino's credit system for credit issuance (i.e. marker) and credit payment (i.e. marker redemption) activities for a customer with large chip or token redemptions. Identification and verification of customers with chip, ticket or token redemptions can be logically integrated with a casino's existing risk-based prevention program for Anti Money Laundering/Combating Financing of Terrorism purposes.

(n) Casinos shall implement procedures and systems to assist in the identification of customers opening multiple accounts or wallets for dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid checks undertaken at a threshold level.

10. ***Reporting Transactions to Financial Intelligence Unit-India:***—

(*a*) Every casino shall report following transactions to Financial Intelligence Unit, India as required by the Rules:

(*i*) All cash transactions of the value of more than Rs. 10 lakhs or its equivalent in foreign currency;

(*ii*) All series of cash transactions integrally connected to each other which have been valued below Rs. 10 lakhs or its equivalent in foreign currency where such series of transactions take place within one calendar month;

(*iii*) Counterfeit currency transactions;

(*iv*) All suspicious transactions whether made in cash or not.

(*b*) Reports required to be sent to Director, Financial Intelligence Unit, India shall be sent at the following address:—

Financial Intelligence Unit-India,

6th Floor, Tower - 2,

Jeewan Bharati Building,

Connaught Place

New Delhi-110001.

(*c*) The transactions required to be reported under sub-clause (*a*) above shall be reported in the form of following reports:-

(*i*) ***Cash Transaction Report (CTR)–***

A report of transactions mentioned at sub—clause (*a*) (*i*) and (*ii*) above of every month by fifteenth day of the succeeding month.

(*ii*) ***Counterfeit Currency Report (CCR)–***

A report of transactions mentioned at sub-clause (*a*) (*iii*) above not later than seven working days from the date of occurrence of such transactions.

(*iii*) ***Suspicious Transaction Report (STR)*** -

A report of transactions mentioned at sub-clause (*a*) (*iv*) above not later than seven working days on being satisfied that the transaction is suspicious.

(*d*) Casinos shall ensure to take appropriate steps to identify suspicious transactions and have appropriate procedure for reporting such transactions.

(*e*) A list of alert indicators for detection of suspicious transactions at casino is given in Schedule hereto. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances. Casinos are also encouraged to apply additional alert indicators to address specific risks faced by them.

(*f*) Employers of the casino shall report any suspicious transactions noticed by them to the Principal Officer of the casino with details of the client, transactions and the nature/reason of suspicion. While determining suspicious transactions, casinos should be guided by definition of "suspicious transaction" contained in the Rules, as amended from time to time.

(*g*) It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. It is clarified that casinos shall report all such attempted transactions in Suspicious Transaction Reports, even if not completed by customers, irrespective of the amount of the transaction.

(*h*) Casinos shall make Suspicious Transaction Reports if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged to predicate offences in part B of the Schedule to the Act.

(*i*) The STR shall be furnished within seven days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion once a STR is received from a branch or any other office. Such report shall be made available to the competent authorities on request.

(*j*) The casinos shall attempt to provide comprehensive information about the ground of suspicion of the suspicious transaction covering the following:

(*i*) Background/profile/occupation of the customer and other related individuals//entities.

(*ii*) When did the relationship with the customer begin?

(*iii*) How was suspicion detected?

(*iv*) What information was linked or collected during the review process?

(*v*) What explanation was provided by the subject(s) or other persons (without tipping off)?

(*vi*) Summary of suspicion.

(*vii*) Whether the suspicious activity is an isolated incident or relates to another transaction?

(*viii*) Who benefited, financially or otherwise, from the transaction(s), how much, and how (if known)?

(*ix*) What is the volume of transactions in a given period and what is the volume of cash transactions?

(*x*) Whether any STR filed for the customer earlier?

(*xi*) Any additional information that might assist law enforcement authorities.

(*k*) Casinos and their employees shall keep the fact of furnishing of Suspicious Transaction Report strictly confidential, as required under the Rules. It shall be ensured that there is no tipping off to the customer at any level.

11. ***Combating Financing of Terrorism.***—

(*a*) According to the Rules, suspicious transaction shall include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

(*b*) Casinos shall regularly download the list of individuals and entities on the list of the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs). The updated list of such individuals/entities can be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml. Casinos shall ensure that the name(s) of the proposed customers does not appear in the list.

12. ***Maintenance of Record.***—

(*a*) Casinos shall ensure compliance with the record keeping requirements contained in the rules, as well as other relevant legislation for the time being in force. Under the Rules, records of identity are required to be maintained for a period of ten years after the cessation of relationship with a client and records of transactions for ten years from the date of transaction.

(*b*) Casinos shall ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities.

(*c*) Casinos shall take appropriate steps to evolve a system for proper maintenance and preservation of customer information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

(*d*) Casinos shall maintain all necessary records of transactions which will permit reconstruction of individual transactions, including the following information:

(*i*) the nature of the transactions;

(*ii*) the amount of the transaction and the currency in which it was denominated;

(*iii*) the date on which the transaction was conducted; and

(*iv*) the parties to the transaction.

(*e*) Casinos shall ensure that all the records pertaining to the identification of the customers are properly preserved for at least ten years after the business relationship is ended as required under rule 10 of the rules. The identification records and transaction data shall be made available to the competent authorities upon request.

(*f*) Casinos shall pay special attention to all complex, unusual, large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/ memorandums pertaining to such transactions and purpose thereof shall, as far as possible, be examined and the findings at branch as well as Principal Officer level shall be properly recorded. Such records and related documents shall be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to other relevant authorities. These records are required to be maintained for a period of five years as is required under section 12 of the Act.

13. ***Audit:***

A casino's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the Know Your Customer policies and procedures. As a general rule, the compliance function shall provide an independent evaluation of the casino's own policies and procedures, including legal and regulatory requirements. Casinos shall ensure that their audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/Internal Auditors shall specifically check and verify the application of Know Your Customer procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard shall be put up before the management at regular intervals.

14. ***Education and Training***:

(*a*) *Customer Education*: Implementation of Know Your Customer procedures requires casinos to demand certain information from customers which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. There is, therefore, a need for casinos to prepare specific literature//pamphlets etc., so as to educate the customer of the objectives of the Know Your Customer programme. The front desk staff needs to be specially trained to handle such situations while dealing with customers.

(*b*) ***Hiring of Employees***: It may be appreciated that Know Your Customer norms/Anti Money Laundering standards/Combating Financing of Terrorism measures have been prescribed to ensure that criminals are not allowed to misuse the casino. It would, therefore, be necessary that adequate screening mechanism is put in place by casinos as an integral part of their recruitment/hiring process of personnel.

(c) ***Employee's Training***: Casinos must have an ongoing employee training programme so that the members of the staff are adequately trained in Know Your Customer procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the Know Your Customer policies and implement them consistently. Casinos shall establish ongoing employee training to ensure that employees are kept informed of new developments, including information on current Money Laundering (ML) and Financing of Terrorism (FT) techniques, methods and trends; and that there is a clear explanation of all aspects of Anti Money Laundering/Combating Financing of Terrorism laws and obligations, and in particular, requirements concerning Customer Due Diligence and suspicious transaction reporting.

PAWAN AWASTHY
Principal Director
Directorate of Sikkim State Lotteries
Government of Sikkim
File No:Fin/Dssl/III/960/2023-24